Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of
Location Based Services (LBS)
WT Docket No. 11-84

Comments of the
Privacy Rights Clearinghouse

July 8, 2011

Introduction

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Federal Communications Commission (FCC) for its consideration with respect to its call for public comment on Location Based Services (LBS) in WT Docket No. 11-84. The FCC's notice in this proceeding solicited written comments in conjunction with a public education forum that was conducted on June 28, 2011. The forum featured representatives of telecommunications carriers, technology companies, consumer advocacy groups and academia.

The PRC is a nonprofit organization, established in 1992 and located in San Diego, California. Our mission is two-part: consumer education and consumer advocacy. We have published more than 50 Fact Sheets that provide practical information consumers may employ to safeguard their personal information, and we invite individuals to contact the organization with their privacy-related questions, concerns and complaints.

Comments

Mobile devices today are powerful computing machines. Many mobile devices run on platforms that allow third-party developers to create software applications (apps) to perform specialized tasks. Two of the most widely used mobile platforms, Apple iOS and Google Android, offer consumers hundreds of thousands of apps to download through the Apple App Store and Android Market. Unlike desktop computers, mobile devices are, by definition, mobile which introduces unique privacy implications for their users. In fact, LBS technology is a major selling point for many mobile devices. / Testimony of Ashkan Soltani before the United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law, Hearing on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy http://judiciary.senate.gov/pdf/11-5-10%20Soltani%20Testimony%20-%20Revised.pdf at 2.

According to an October 2010 study by the Pew Institute, 85% of the U.S. adult population owns a cellular phone. http://pewinternet.org/Reports/2010/Gadgets/Report/Findings.aspx (accessed July 7, 2011). The proliferation of cell phones, other mobile devices, and mobile Internet devices (including tablets and laptops), along with federal E911 requirements and the ubiquity of GPS-

capabilities in mobile devices have spurred the development of location-sharing applications. These LBS technologies typically allow users to share their real-time or historical location information online.

The process by which location providers gather location data has always raised significant privacy concerns. Location providers have now begun using their customers' devices in order to compile databases of the physical locations of wireless landmarks. This "crowdsourcing" of location data has introduced additional privacy concerns. By leveraging consumers' mobile devices, location providers receive the location of the mobile device as they report their findings. / Testimony of Ashkan Soltani before the United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law, Hearing on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy http://judiciary.senate.gov/pdf/11-5-10%20Soltani%20Testimony%20-%20Revised.pdf at 4.

Several specific examples of LBS technology facilitating privacy abuses have been reported within the past year:

- In December 2010, an investigation by the Wall Street Journal (WSJ) revealed that of 101 top apps for Apple iPhones and Google Android smartphones, 47 disclosed a user's location to third parties without his or her consent. http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html (accessed July 7, 2011).

- Another WSJ investigation in April 2011 revealed that Apple iPhone and Google Android smartphones were automatically sending Apple and Google information about the smartphone's whereabouts—even when users were not using location applications and, in Apple's case, even though users had no way to stop this collection. http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html (accessed July 7, 2011).

- In April 2011, two researchers announced that iPhones, and 3G iPads regularly record the position of the iOS device into a hidden file. An iOS 4 software update began storing a list of locations and time stamps. This database is restored across backups and device migrations. The file is unencrypted and resides on any machine that has synched with the iOS device. It can also be easily accessed on the iOS device itself if it falls into the wrong hands. Anybody with access to this file can determine the device's location at any time since iOS 4 update was released. http://radar.oreilly.com/2011/04/apple-location-tracking.html (accessed July 7, 2011).

- A May 2011 Future of Privacy Forum analysis of the top 30 paid mobile apps across the leading operating systems (iOS, Android, and Blackberry) found that 22 out of the top 30 applications lacked even a basic privacy policy. http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/ (accessed July 7, 2011).

Events such as these have raised serious concerns among the American public about their locational privacy on cell phones, smartphones, and other mobile devices. Indeed, a January 2011 survey by Microsoft revealed that 84% of respondents were concerned about sharing of their location data without their consent, 84% were concerned about identity theft or data theft, and 83% were concerned about loss of privacy. Forty-nine percent would be more comfortable with LBS if they could easily and clearly manage who sees their location information. The key takeaway is that while people can see the benefits of LBS, they are concerned about their privacy and are eager for greater transparency and control over how their location information is used and shared. http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/01/26/location-and-privacy-where-are-we-headed-on-data-privacy-day-natural-user-interface.aspx (accessed July 7, 2011).

A Spring 2011 nationwide survey of 1,000 smartphone users conducted by Harris Interactive for TRUSTe explored consumers' mobile privacy attitudes and concerns. It also identified areas needing greater privacy protections through increased transparency, accountability and choice. The vast majority of survey respondents (98%) believed that privacy is an important issue when using a mobile device and wanted more transparency and choice over the personal information mobile apps and websites collect and share, especially as it relates to targeted advertising and geo-location data. Additionally, 38% of individuals identified privacy as their number one concern when using mobile applications, followed by security (26%) and identity tracking (19%). http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/index.html (accessed July 7, 2011).

Additional findings in the Harris Interactive survey included:

- Individuals are wary of ad targeting and they want opt-out ability. Nearly three-quarters are uncomfortable with the idea of advertiser tracking, and 85% want to be able to opt in or out of targeted mobile ads.

- Lack of consumer choice may heighten concerns with LBS. Only 36% of individuals feel they have a choice regarding the collection and use of their location information, which may explain why 40% report that they purposefully do not share location data with mobile applications.

- Individuals clearly desire transparency and choice. 74% of consumers believe it's "very important" or "extremely important" to understand what personal information a mobile app collects, and 98% of consumers believe it's important for mobile apps to provide easy access to controls for collecting and sharing personal information.

http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/index.html (accessed July 7, 2011).

Unlike other information in cyberspace, an additional concern with LBS data is that such data has the potential to allow an adversary to physically locate a person. Therefore, many individuals, such as victims of stalking and domestic violence, have legitimate concerns about their personal safety in the event that LBS information falls into the wrong hands.

It is important to note that apps are generally written by service providers rather than by carriers. From a business standpoint, it is in the best interest of a service provider to obtain as much information about a user as is possible. Consequently, there are built-in incentives for apps to collect LBS information without regard to users' privacy interests.

Researchers at Carnegie Mellon University have demonstrated that the primary dimensions of privacy concern surrounding the disclosure of this information include context and use. The willingness to share one's location and the level of detail shared depends highly on who is requesting this information and the social context of the request. Because users' varied privacy concerns and preferences are situational depending on the activity in which the user may be engaged, privacy controls need to be flexible.

In addition to the context of a location request, it is individuals' own perceptions of the use of one's location information that impacts their privacy concerns. For example, a user may be more concerned with an acquaintance requesting his or her location (because they are unsure of why that information is being requested) compared to users' lack of concern when sharing location information with people nearby to find restaurant recommendations. / Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (Carnegie Mellon University, February 2010) http://www.normsadeh.com/file_download/37/TsaiKelleyCranorSadeh_2009.pdf at 5.

The top ranked expected risks are the following:

- Revealing the location of your home to people you do not want knowing your address.
- Being stalked.
- Having people intrude on your private space.
- Being found by someone you don't want to see.
- Being found when you want to be alone.
- Having the government track you.
- Being targeted by ads that use your location.

Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (Carnegie Mellon University, February 2010) http://www.normsadeh.com/file_download/37/TsaiKelleyCranorSadeh_2009.pdf at 17.

To address consumers' privacy concerns, the International Association for the Wireless Telecommunications Industry (CTIA), issued Best Practices and Guidelines for LBS providers. These guidelines are meant to help LBS providers protect user privacy and rely in part upon two of the Fair Information Principles (FIPs) -- user notice and consent (Fair Information Practice Principles, Federal Trade Commission http://www.ftc.gov/reports/privacy3/fairinfo.shtm) (accessed July 7, 2011).

The CTIA's guidelines include the following:

- LBS providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected so that users can make informed decisions whether or not to use the LBS and thus will have control over their location information.

- LBS providers that want to use location information for a new or materially different purpose not disclosed in the original notice, they must provide users with further notice and obtain consent to the new or other use.

- LBS providers must inform users how long any location information will be retained, if at all.

- LBS providers that share location information with third parties must disclose what information will be provided and to what types of third parties so that users can understand what risks may be associated with such disclosure.

- LBS providers must periodically remind users when their location information may be shared with others and of the users' location privacy options, if any.

- LBS providers must ensure that users consent to the use or disclosure of location information, and LBS providers bear the burden of demonstrating such consent.

- LBS providers must allow users to revoke their prior consent to use or disclose location information to all or specified groups or persons.

- LBS providers must employ reasonable administrative, physical and/or technical safeguards to protect a user's location information from unauthorized access, alteration, destruction, use or disclosure. LBS providers should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.

- LBS providers should retain user location information only as long as business needs require, and then must destroy or render unreadable such information on disposal.

CTIA, Best Practices and Guidelines for Location Based Services (Version 2.0, effective March 23, 2010) http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf.

The CTIA's voluntary guidelines, if adopted by LBS providers, represent a good first step toward protecting consumers of LBS services. However, reliance upon voluntary industry guidelines, without any mandatory direction from regulatory agencies, fails to provide adequate protection for LBS users.

Conclusion

As mobile devices become more powerful, information from LBS technology becomes a more valuable asset for commercial endeavors. Consumers continue to express significant concerns about how their mobile devices expose their personal information, often in unexpected ways. Individuals must be able to trust their devices – and the myriad of features and tools provided by them -- in order to fully utilize the benefits of LBS technology.

PRC recommends that the FCC institute a rulemaking proceeding in conjunction with the Federal Trade Commission (FTC) to promulgate regulations that will protect consumers' privacy interests when using LBS technology. These regulations should be guided by a strong set of Fair Information Principles (FIPs), with the principle of opt-in as the foundation.

Two examples of robust FIPs are the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html and the U.S. Department of Homeland Security's *Fair Information Practice Principles* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. Another useful set of FIPs forms the basis of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) http://www.priv.gc.ca/leg_c/p_principle_e.cfm#contenttop. (accessed July 8, 2011)

Reliance upon voluntary industry guidelines is simply insufficient, since there is little incentive for industry to comply with such guidelines, and no penalty for failure to comply.

Well-drafted regulations will play a significant role in the development of LBS technology by providing clear guidance to the industry about what they may or may not do. Telecommunications carriers, third-party app developers and other businesses have a strong interest in developing new LBS services, and consumers have a strong interest in protecting their privacy. Regulations specifying how individuals authorize access to their location information must be clear and user-friendly.

Regulations concerning the collection, storage and sharing of location information could in fact legitimize services that might previously have alarmed consumers. Accordingly, regulation can be viewed not only as privacy-enhancing, but supportive of industry efforts to roll out additional LBS services. With regulations providing greater control over their privacy, individuals will feel more comfortable enjoying the benefits of LBS technology while at the same time steering clear of the risks that could come with the use of LBS.

Respectfully Submitted,

Beth Givens, Director
Privacy Rights Clearinghouse
3100 5th Ave., Suite B
San Diego, CA 92103
www.privacyrights.org